TECHNOLOGY RESOURCES AND DATA MANAGEMENT

The Board of Education (the Board) of the Bethlehem Central School District (the District) recognizes that computers, computer networks, and other technological resources are needed for instruction, as well as management of District business. The Board also recognizes that District Technology is used to create, store, and transfer data created by students, staff, and other authorized users. This Technology Resources and Data Management Policy sets forth the Board’s expectations regarding management of District Technology and Data.

Definitions

A. “District Technology” includes:
   1. All District-owned, leased, or controlled computer equipment, software, applications, and other electronic devices (including, but not limited to, Chromebooks, laptops, smartphones, databases, webpages, and email accounts, social media accounts, etc.);
   2. The District’s computer network, including network components located on school premises and remote components, such as District-authorized cloud storage solutions (e.g., Google Classroom); and
   3. District-owned, leased, or controlled wired and wireless connections used to access the District’s computer network or the internet.

B. “Data” includes:
   1. Data accessed, created, compiled, stored, or maintained on District Technology, regardless of whether such Data was created for District purposes and regardless of who owns the legal rights to such Data; and
   2. Data accessed, created, compiled, stored, or maintained on any District-authorized cloud storage solution, regardless of whether such Data was created for District purposes and regardless of who owns the legal rights to such Data.

C. “Personal Device” includes any computing device not owned, leased, or controlled by the District.

D. “User” includes any person who is authorized to access District Technology or Data, including students, staff, Board members, contractors, and visitors.

Management Responsibilities

A. The superintendent is responsible for designating a Director of Technology (DOT) to oversee the installation, use, management, and disposal of District Technology and Data.

B. The superintendent, working in conjunction with the designated purchasing agent for the District and the DOT, is responsible for:
   1. Preparing a comprehensive multiyear technology plan for Board approval, which may be revised from time to time (subject to Board approval) to reflect changing technology and District needs;
2. Purchasing, distributing, and/or installing District Technology pursuant to the Board-approved technology plan, including devices that may be issued directly to students for their use both in school and outside of school;
3. Adopting reasonable and appropriate procedures relating to the access, use, storage, and disposal of District Technology and Data;
4. Adopting reasonable and appropriate internet filtering technologies required to comply with the District’s Internet Safety Policy and Regulation (4526.1/4526.1-R);
5. Adopting reasonable and appropriate technical, administrative, and physical safeguards to protect the confidentiality, integrity, and availability of District Technology and Data;
6. Preparing reasonable and appropriate notices and training programs for Users relating to appropriate use of District Technology, Data, and Internet Safety;
7. Adopting reasonable procedures to create and manage administrative and individual User accounts, including maintaining District access rights to all such accounts;
8. Implementation of all other District policies relating to District Technology and Data, including but not necessarily limited to:
   a. Policy No. 4526 and Regulation No. 4526-R concerning Acceptable Use of District Technology;
   b. Policy No. 4526.1 and Regulation No. 4526.1-R concerning Internet Safety; and
   c. Policy No. 8635 and Regulation No. 8635-R concerning Information Security
      Breach and Notification.

User Rights and Limitation of District Obligations

A. No Expectation of Privacy. Users have no expectation of privacy regarding use of District Technology or storage of Data on District Technology, including, but not limited to, Data contained in any User account, on the District’s computer network, on any authorized cloud computing solution, or on any device issued by the District to any student, staff member, or other person.

B. No Warranties. The District makes no warranties of any kind, express or implied, relating to access to, or use of, District Technology or Data. Further, the District assumes no responsibility for the quality, availability, accuracy, nature, or reliability of the service and/or information provided. Users of District Technology use such technology at their own risk. Each User must understand that information obtained from the internet or other online sources is not necessarily reliable and the User is solely responsible for any subsequent use of information obtained from the internet or other online source.

C. Limits on Filtering Technology. No internet filtering/blocking software is 100 percent effective. The District is not responsible for the failure of such software to block or prevent access to all potentially objectionable content.
D. *Limits on Security Controls.* No security controls are 100 percent effective to eliminate all threats. The District is not responsible for the failure of any reasonable security controls to preserve the confidentiality, integrity, and availability of District Technology or Data.

Cross-Reference: 1130.1 Social Media Guidelines
4526 Acceptable Use
4526.1 Internet Safety
8635 Information Security Breach and Notification

*Adoption date:* August 9, 2017
*Revised date:* September 23, 2019
*Re-Adopted:* October 16, 2019